CHALLENGES IN THE PROTECTION OF US CRITICAL INFRASTRUCTURE IN THE CYBER REALM

A Monograph

by

Lieutenant Colonel (GS) Jan Trobisch
German Armed Forces

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2014-01

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ORGANIZATION.

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
22-05-2014	Master's Thesis	JUL 2013 - MAY 2014

4. TITLE AND SUBTITLE

CHALLENGES IN THE PROTECTION OF US CRITICAL INFRASTRUCTURE IN THE CYBER REALM

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

JAN TROBISCH
LIEUTENANT COLONEL, German Armed Forces
Infantry/Special Forces

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
100 Stimson Ave.
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This paper evaluates the US military participation in the arena of domestic cyber security for critical infrastructure protection. The issue is relevant for two major reasons. First, it deals with the current phenomena of continuous cyber attacks on US critical infrastructure, which dominates the discussion of potential future and global threats to the United States. Second, the US is trying to cope with current challenges to cyber security with military means, which is sparking academic and political debate. The latter relevance comprises the main argument of this study, that a military approach to cyber security is not the best choice. Generally, critical infrastructure protection is inherently civil related. Nonetheless, the US military is deeply involved in domestic affairs regarding cyber security. Numerous reasons create this curious reality. The absorption of DHS related fields of actions by the Department of Defense are questionable in two respects: constitutionally power-sharing principles prohibit the military from policing inside of the United States and the militarization of cyber security may hamper the necessary public-private cooperation for domestic cyber security.

15. SUBJECT TERMS

Cyber security, Critical Infrastructure, Department of Homeland Security, Cyber hype, Cyber defence, Cyber protection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(Include area code)*
Unclassified	Unclassified	Unclassified	UU	53	

Reset

MONOGRAPH APPROVAL PAGE

Name of Candidate: Lieutenant Colonel (GS) Jan Trobisch

Monograph Title: Challenges in the Protection of US Critical Infrastructure in the Cyber Realm

Approved by:

_____, Monograph Director
Jeffrey J. Kubiak, Ph.D.

_____, Seminar Leader
Charles M. Evan, COL, FA

_____, Director, School of Advanced Military Studies
Henry A. Arnold III, COL, IN

Accepted this 22nd day of May 2014 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, Ph.D.

ABSTRACT

CHALLENGES IN THE PROTECTION OF US CRITICAL INFRASTRUCTURE IN THE CYBER REALM by Lieutenant Colonel (GS) Jan Trobisch, 45 pages.

This paper evaluates the US military participation in the arena of domestic cyber security for critical infrastructure protection. The issue is relevant for two major reasons. First, it deals with the current phenomena of continuous cyber attacks on US critical infrastructure, which dominates the discussion of potential future and global threats to the United States. Second, the US is trying to cope with current challenges to cyber security with military means, which is sparking academic and political debate. The latter relevance comprises the main argument of this study, that a military approach to cyber security is not the best choice. Generally, critical infrastructure protection is inherently civil related. Other factors to consider are Presidential Directives and US cyber strategies, which assigned the Department of Homeland Security (DHS) to organizing, synchronizing, and executing critical infrastructure protection for the homeland. Nonetheless, the US military is deeply involved in domestic affairs regarding cyber security. Numerous reasons create this curious reality. Ill-defined and unclear classifications of the variety of cyber attacks make almost everything appear as an undifferentiated hazard. Cyber hype, largely a product of efforts by the information technology industry, only serves to add to the contemporary misperception of cyber threats. Terms of cyber related issues are often militarized, over emphasized, and undifferentiated. The resulting confusion produced inadequate domestic cyber security efforts, insufficient public-private cooperation, and a turn to the military for leadership. This absorption of DHS related fields of actions by the Department of Defense are questionable in two respects: constitutionally power-sharing principles prohibit the military from policing inside of the United States and the militarization of cyber security may hamper the necessary public-private cooperation for domestic cyber security.

ACRONYMS

CCDCOE	Cyber Defense Centre of Excellence
CNA	Computer Network Attack
DHS	Department of Homeland Security
DOD	Department of Defense
FISA	Foreign Intelligence Surveillance Act
FISAAA	FISA Amendment Act
GDP	Gross Domestic Products
ICS	industrial control system
ICT	information communications technology
IP	Internet protocols
ISACs	Information Sharing and Analysis Centers
ISO	International Organization of Standardization
IT	information technology
NATO	North Atlantic Treaty Organization
NSA	National Security Agency
PDD	Presidential Decision Directive
SAIC	Science Applications International Corporation
SIGINT	Signal Intelligence
SLTT	state, local, tribal, and territorial entities
SSAs	Sector-Specific-Agencies
USG	United States government

TABLE OF CONTENTS

ILLUSTRATIONS

Page

INTRODUCTION

> The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.[1]
>
> —Sun Tzu, *Art of War*

People depend on information and communications infrastructure for governing societies, conducting business, and exercising basic understanding between interconnected human beings. Similarly, nations have become dependent on information and communications infrastructure. Threats against its availability, integrity, and confidentiality affect the very functioning of societies. Access to the cyber realm is a key issue of the 21st century. As part of an increasingly networked world, the state, critical infrastructure, economy, and population depend on the reliable functioning of information and communication technology (ICT) as well as the Internet. Defective information technology (IT) products and components, a breakdown of information infrastructures, or severe attacks in the cyber realm can have a serious impact on technical, economic, and administrative efficiency impacting the very social foundations of the state's existence. Unauthorized access, manipulation of data and networks, and destruction of critical resources also threatens the integrity and resilience of critical core societal infrastructure. The proliferation and replication of malicious software like Stuxnet, Flame, and Duqu that can penetrate and establish control over remote systems is alarming. Moreover, cyber attacks constantly take place, both by state and non-state actors.[2] Catastrophic cyber threat scenarios predict a world where attackers would plunge cities into darkness, manipulate power grids, damage water supplies, and cause severe traffic accidents. Nevertheless, no attack—and there

---

[1]Sun Tzu, *The Art of War (History and Warfare)* (Boulder: Basic Books, 1994), 203-204.

[2]US Department of Homeland Security, "ICS-CERT Year in Review—2012: Industrial Control Systems Cyber Emergency Response Team," 2012, 12-14, http://ics-cert.us-cert.gov/sites/default/files/documents/Year_in_Review_FY2012_Final.pdf (accessed 9 April 2014).

were over ten thousand cyber attacks in the last decade—has produced such results. Prognostications arose from a lack of insight into the capabilities of cyber-attacks and from an overestimation of both the likelihood of complex cyber-attacks as well as the power of cyber as a weapon. Regardless of the lack of evidence of a catastrophic cyber attack and the overestimation of potential damage that would result, there is still a real threat that must be addressed.

The resultant cyber security issues challenge everyone. This prompts the question, what is the nature of the US military participation within the realm of cyber security? Although the cyber threat problem seems obvious, the extensive discourse in the literature shows a wide range of ideas and little agreement on the topic. There seems little consensus about the meaning, importance, and consequences of cyber threats. Missing, non-standardized, and unclear definitions on the subject further complicate the understanding of the cyber realm. A common knowledge would help produce common understanding and distinguish specific cyber threats from other threats in order to examine problems. The military related spectrum of cyber is cyber warfare, the most recent form of warfare. It is inherently a technologically oriented approach to war. Due to its relative infancy as a form of warfare, it is plagued by a plethora of confusing definitions, conflicting interpretations, and predictions regarding its future application. The current literature on cyber warfare covers a mix of poorly differentiated issues including cyber-crime, electronic warfare, information warfare, hacking, and cyber-terrorism, just to name a few. The results of this mixture describe worst-case scenarios in which everything is possible in war and warfare.[3]

The subsequent challenge, given unclear definitions of the threat, is the need to map a clear way forward on cyber. The existence of different factions with contending and assumption-

[3]Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1989), 75, 95. War is an event through physical force, like a duel on a larger scale to compel the opposing party to do the antagonist´s will. Warfare comprises everything related to the fighting forces – everything to do with their creation, maintenance, and use.

based beliefs of what cyber actually is, how dangerous cyber threats to critical infrastructure are, and what kind of consequences (actions or precautions?) should be taken provide multiple approaches to the problem. Moreover, there is a diverse body of literature available whose origin and motivation should be examined closely. Many think-tank papers are the result of ordered and commissioned studies by governmental entities or private business consortia.[4] Motivations of those researchers are different from the independent researcher. Even military papers may have tendencies for bias. For example, military arguments articulate cyber activities (in a defensive and offensive role) as extended features of military actions.[5] It is particularly serious if "military experts" proclaim cyber activities as a new kind of war, or a revolution of military affairs, take it out of context and away from generally accepted theories of war.

It seems that cyber threats, at first glance, are complex and uncontrollable. The mixture of meanings and definitions results in an overwhelming doom-scenario. Additionally, these scenarios raise a serious challenge for democratic states. They must cope with threats to a range of public and private interests involving power-sharing governmental agencies, private entities, and the society. This study seeks to understand the cyber threat through an examination of the components of attacking, protecting, and defending US critical infrastructures. It uses the example of the United States as a basis of understanding the different developments of governmental organizations to cope with the situation. Such an analysis contributes to the existing body of literature by suggesting a new perspective for understanding the variety of cyber security

[4]US government and private endowment financed think tanks such as RAND Cooperation and CSIS, which published amounts of studies about cyber, seem very popular.

[5]Benjamin S. Lambeth, "Airpower, Spacepower, and Cyberpower" *Joint Force Quarterly* (2011): 46-53, http://www.ndu.edu/press/lib/images/jfq-60/JFQ60_46-53_Lambeth.pdf (accessed 12 February 2014). One example among others describes the necessity of extensive cyber capability within the military to maintain the international supremacy of the US military.

responsibilities of various governmental agencies and shaping the future of organizational roles in the realms of cyber security.

The first purpose of this study is to find clearer definitions of relevant terms. It is the starting point for a better contextual understanding of cyber threats against US critical infrastructure and any effort to identify the scope of cyber security measures. A second purpose is to explore the significance of critical infrastructure to determine different responsibilities to protect, secure, and finally defend this object. Thirdly, this study determines how different perceptions of cyber threats influence institutional understanding of governmental agencies. Lastly, an analysis of the current state of development of governmental organizations related to cyber and their correlations to each other that symbolize a construct of perceptions. Each agency´s perception affects its role and responsibility. This clarifies the confusion regarding cyber terminology, the description of original responsibilities to cyber threats on the national level, and demonstrates how misperceptions and challenges to achieve the assigned goals result in a diffusion of actions. The current organizational development has the potential to endanger the entire goal and may steer the military into an undesired direction. The key argument in this study is that the military should not play a central role in protecting critical infrastructure; that its role should be tangential. Therefore, military professionals and policy makers are the intended audience for this study.

It is beyond the scope of this paper to provide a detailed view on all cyber activities, capabilities, and analysis of different threat scenarios. Generally, this study will refrain from overly sensationalized views of cyber threats. Although the risk of a debilitating cyber attack exists in the theoretical, the perception of its likelihood is far greater than it actually occurring. Key points include a description of the general cyber threat or challenge and possible risks to critical infrastructures as a precondition for using strategic roles and advantages from a state perspective. Another limitation on the research is the state of current literature on cyber security

measures and concepts. To mitigate impacts from the expansive and disconnected literature, this work provides a general view of cyber issues holistically without a separate analysis of each specific national security concept. It is more important for the purpose of this monograph to provide perspectives on how US agencies understand their own responsibility within this realm. In accordance with the context of this study, there will be no deep analysis or insights on operational or tactical cyber employment.

In order to address the question of the nature of US military participation within the realm of cyber security; this study demonstrates that the US military, as the representative instrument of the Department of Defense, must take a tangential role in domestic cyber security. The over-militarization of cyber security, due to poorly defined terminology and augmented by the negative aspects of cyber hype, violates constitutional separation between the Department of Defense and Department of Homeland Security. This is counter-productive to creating a whole-of-nation approach between the public and private sector.

The methodology employed in this study will be based largely on deductive reasoning. First, in providing definitions about terms (Section 1) this study will confine its discussion to those cyber threats that endanger a state´s critical infrastructure, dividing it from other non-significant spectrums of cyber threats. This section establishes that in this modern age the importance of information and communication technology and their relation to vital critical infrastructure is important for analysis. It examines the vulnerabilities and risks of the critical infrastructure from a cyber point of view. This approach allows for filtering the different levels of responsibilities to provide security and demonstrates the challenges of US governmental agencies in achieving their assigned goals.

US government policy provides a relatively clear vision for cyber strategies. The objective of cyber security is to defeat cyber threats and maintain the strategic advantage for the

United States in the future.[6] In achieving this vision, the United States government (USG) assigned one specific department, the Department of Homeland Security (DHS), to coordinate a comprehensive effort to protect against domestic cyber threats, which includes the entire spectrum of public and private agencies and agents within the US This study analyzes the approach by examining two different sets of variables: (1) the institutional aspects, looking at how the effort is institutionally organized, and (2) the cognitive factors, which influence the perceptions of cyber threats in the United States. Finally, this study combines the results of the analysis of institutional challenges with the influence of cognitive factors in order to generate a better understanding of cyber security in the United States.

DISAMBIGUATION OF CYBER REALM, CYBER SECURITY, CYBER ACTIVITIES

To date, there is not a universal understanding of basic cyber terms and definitions, so common solutions remain scarce. Definitions of terms referencing cyber realm are varied because of different perspectives of meanings and purposes. Governmental papers define what they mean by cyber realm according to their individual cyber strategies. In contrast, private entities refer their definitions to identified vulnerabilities and opportunities.[7] In this section, a thorough

---

[6]White House, "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009," http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 10 February 2014).

[7]There are two contrasting examples with different assessments of cyber security for business available: (1) Lane F. Cooper, "Cyber Security Strategies for the Small Businesses Market," *Solutions for Small Business Reports* (2010), http://www.ctam.com/html/sfsb/pdf/Security-White-Paper.pdf (accessed 18 November 2013). Cyber Security Strategies for the Small Businesses Market, which described cyber security more from a technical aspect. (2) Geoff Smith, "Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy," *OECD paper* (2010), http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf (accessed 18 November 2013). In a much bigger scope, an OCED study addressing big Internet operating companies and analyzing national cyber security strategies of ten different countries, and how important cyber security is for protecting national economic power.

demonstration of definitions illustrates a generalizing and simplifying approach. The purpose is to illustrate the scope of cyber rather than a deep analysis of technical details.

The Internet is a critical national resource for governments, a vital part of national infrastructures, and a key driver of socio-economic growth and development. In some countries, the Internet contributes up to eight percent of gross domestic product (GDP) and the G20 has established goals to increase the Internet's contribution to GDP.[8] The cyber realm´s value and potential is nurtured by private and public sector investments in high-speed broadband networks and affordable mobile internet access, as well as innovations in computing power, smart power grids, cloud computing, industrial automation networks, intelligent transport systems, electronic banking, mobile e-commerce, social nets, and many other sectors.[9]

Modern business hardware and software enable communication with the Internet. The key element is an industrial control system (ICS) that monitors, processes, and controls the flow and availability of information. Its functionality is like an on or off feature. An ICS is able to control the entire process within a system such as the flow of natural gas to a power generation facility, the flow of electric grids, or the functionality of traffic control centers. Over the last decade, industry has increased connections within and between critical infrastructures and their control system networks.[10]

---

[8]David Dean et al., "The connected world: The digital manifesto: How companies and countries can win in the digital economy," *Boston Consulting Group Perspectives* (BCG), (27 January 2012): 1, https://www.bcgperspectives.com/content/articles/growth_innovation_connected_world_digital_manifesto/ (accessed October 2013).

[9]Alexander Klimburg, ed., *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn (2012): 2, http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (accessed 13 October 2013).

[10]Ibid., 3.

The rise of the Internet, and the increasing social, economic, governmental dependence on it, will increase in the near future. As the Internet becomes increasingly important, threats to it become more dangerous. (See figure 1.)

	Today	2020
Estimated World Population	7 billion people	~8 billion people
Estimated Internet Population	2.5 billion people (35% of population is online)	~5 billion people (60% of population is online)
Total Number of Devices	12.5 billion internet connected physical objects and devices (~6 devices per person)	50 billion internet connected physical objects and devices (~10 devices per person)
ICT Contribution to the Economy	~4% of GDP on average for G20 nations	10% of worldwide GDP (and perhaps more for developing nations)

Figure 1. Internet: Today and the Near Future

Source: Alexander Klimburg, ed., *National Cyber Security Framework Manual* (NATO CCD COE Publication, Tallinn 2012), 4, Table 2.

The Internet, the ICS, networks, and different types of network-based interactions, operating with software and hardware, comprise the cyber realm. Cyber realm virtually and physically exists with resulting virtual and physical effects. As noted above, cyber realm´s importance is closely linked to its vulnerability, under considerable threat in multidimensional ways, in various degrees and forms, and for varying motivations. Current threats and sources of cyber realm attacks (a cyber attack occurs if a threat successfully breaches security controls) comprises six groups: (1) foreign intelligence services, (2) organized crime groups,

(3) “hacktivists”, (4) extremist organizations, (5) investigative journalists, (6) disaffected employees.[11]

Cyber Security

The number of cyber security incidents reported by federal agencies continues to rise. Over the past six years the number of incidents reported by US federal agencies has increased nearly 680 percent. These incidents include unauthorized access to systems, improper use of computing resources, and the installation of malicious software among others.[12] In 2009, President Barack Obama declared the cyber threat to be one of the most serious economic and national security challenges and stated that America’s economic prosperity in the 21st century will depend on cyber security.[13]

Experts use a confusing spectrum of definitions, understandings, and meanings when describing cyber security. This is because of the different interpretation of interrelated causes and effects and a different perception about the scope of the threat, ways of thinking, and threat awareness. In light of these confusing definitions, can a holistic approach to cyber security be derived? A common problem with current definitions is the inappropriate distribution of cyber security to individual sub segments such as computers, control systems, Internet, networks, affected organizations, companies, and states. Cyber realm and its security is more than the listed above and should include holistic definitions that include hardware, software and information systems including people and social interactions within these networks. Systems thinking

---

[11]“ITU National Cybersecurity Strategy Guide,” *International Communication Union* (ITU), Geneva: ITU (2011): 13-17, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf. (accessed 22 October 2013).

[12]US Government Accountability Office (GAO), *Cybersecurity, Threats Impacting the Nation*, 24 April 2012, http://www.gao.gov/assets/600/590368.pdf (accessed 22 October 2013), 1.

[13]US Government Accountability Office (GAO), *Cybersecurity, a better defined and implemented national strategy is needed to address persistent challenges,* 7 March 2013, http://www.gao.gov/assets/660/652817.pdf (accessed 22 October 2013), 2.

approach is better able to encapsulate the scope of cyber security related to cyber realm than detailed and micro viewed explanations of sub segments. Therefore, this study uses a combination of two definitions as the most appropriate explanations.

International Organization for Standardization (ISO) defines cyber security as a "preservation of confidentiality, integrity, and availability of information in the Cyberspace."[14] A foreign strategy paper (United Kingdom, 2009) explicitly mentions the cyber realm as all forms of networked, digital activities; this includes the content of and actions conducted through digital networks.[15] By adding the phrase, "the content of, and actions conducted through,' a systems approach can also include relevant human behaviors.

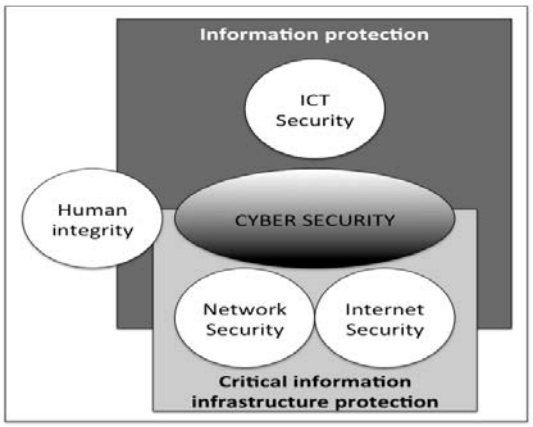

Figure 2. Cyber Security and Security Domains

Source: Alexander Klimburg, ed., *National Cyber Security Framework Manual* (NATO CCD COE Publication, Tallinn 2012), 10.

[14]"Information Technology—Security Techniques—Guidelines for Cybersecurity," *ISO/IEC 27032:2012*, http://www.iso27001security.com, http://www.iso27001security.com/html/27032.html (accessed 11 February 2014).

[15]UK Office of Cyber Security, "Cyber Security Strategy of the United Kingdom, Safety, Security and Resilience in Cyber Space," (June 2009), http://www.official-documents.gov.uk, http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (accessed 10 January 2014).

The preceding paragraph established understanding of the fundamentals of the cyber realm, which allows a realistic threat assessment in the final part of this section. In general, ICT security is directly associated with the technical origins of computer security and 'information security principles', including the confidentiality, integrity, and availability of information resident on a particular computer system.[16] ICT security extends beyond devices that are connected to the Internet to include computer systems that are not connected to the Internet. Malicious or untrustworthy ICT could disrupt the performance of sensitive national information, economic security systems, and compromise essential critical services. The ICT supply chain consists of many phases; design, manufacture, integrate, distribute, install and operate, maintain, and decommission. The highest risk factors in the supply chain are 'after build' (i.e., during the install and operate and retire phases) because this is where multiple vendors participate in the process (e.g., integration, updating, and maintenance). There are few measures to monitor and assure integrity throughout the entire process. This is a problem for all potential endangered entities: the evolution of the ICT industry means that many countries and global corporations now play a role in the ICT supply chain, and no entity can source all components from totally trusted providers. This trust is needed, however, as the promise of ICT-driven economic growth is dependent upon the core infrastructure being both secure and resilient.[17]

A network is a connection of more than two devices, which is developed for communication. A network can operate as a closed system without links to the Internet or an open system with connection to the World Wide Web. Network security concepts, managed by network administrations, ensure protection of unauthorized access and a secure flow of

---

[16]National Institute of Standards and Technology, "Minimum Security Requirements for Federal Information and Information Systems," http://csrc.nist.gov/ publications/fips/fips200/ FIPS-200-final-march.pdf (accessed 11 February 2014).

[17]Klimburg, *National Cyber Security Framework Manual*, 9-11.

information within the network. Network security focuses on the design, implementation, and operation of networks for achieving the purposes of information security on networks within organizations, between organizations, and between organizations and users.[18] An organization´s efficiency and productivity depends on the security of their networks. The protection of networks is especially important for cyber security. Innumerable computer network breaches demonstrate the extent of current cyber threats. Consequences from growing and rapidly changing risks to network-operating systems affect both the economy and separate government organizations. There are a variety of different risks. The human factor, as an integral part of networks, causes a wide range of risks. Password security, cyber awareness, and whistle blower activities are few of large numbers of different risk factors within network-operating systems. External risks exist due to the networks connections to the Internet, malicious ICT within networks, and maliciously installed network technologies (e.g. wiretapping).

Within a technical context, Internet security is concerned with safeguarding internet-related services and associated ICT systems and networks as an extension of network security in organizations and at home to achieve the purpose of security. Internet security also ensures the availability and reliability of Internet services.[19] Internet security does not include non-internet relevant technical issues, including those that address the various 'internets', which are not connected to the World Wide Web. These, however, are covered by the term 'network security'. Critical infrastructure not directly connected to the Internet needs network security.[20]

---

[18]International Standard, ISO/IEC 18028-1. Information Technology—Security Techniques—IT Network Security: Part: 1 Network Security Management (Geneva: www.iso.org, 2006), 44-46, http://www.pqm-online.com/assets/files/standards/iso-iec_18028-1-2006.pdf (accessed March 14, 2014).

[19]Information Technology—Security Techniques—Guidelines for Cybersecurity," ISO/IEC 27032:2012, http://www.iso27001security.com/ html/27032.html (accessed 11 February 2014).

[20]Klimburg, *National Cyber Security Framework Manual*, 11.

It is important to point out the significance of the human factor. Large commercial and private Internet security companies present security as technological problems easily solved with more technology or software. However, expecting technology alone to solve the problem is just one of three dangerous misconceptions about digital security. Improving security means implementing appropriate policies, removing perverse incentives, and managing risks, not just implementing refined hardware and software. The human operator could potentially be the weakest link in cyber security chain. Wrongful behavior of individual users, their failure to comply with security policies and lack of awareness on existing cyber threats represent the main factors that risk the overall integrity of an IT solution.

The human factor is the underlying reason why many cyber attacks are successful; underestimation of the severity of potential cyber threats is one of the most common errors. Social networks can be a virtual goldmine of information and knowledge for those who can potentially harvest it for malicious purposes. The human factor in overall security is determinant; users have to carefully manage the exposition of their data on-line. A wrongful usage of social networking information could damage the user itself, but also other accounts linked to him.[21]

Cyber Crime, Hacktivism, Cyber Espionnage, Cyber Warfare

Without anticipating the meaning of cyber warfare in this section, it has to be stated that hostile and illegal activities in cyber realm are inherently attacks. Differences between cyber crime, cyber espionage, and cyber warfare are mainly related to different actors and entities and their motivations or purposes.

---

[21]Pierluigi Paganinip, "Why Humans Could Be the Weakest Link in Cyber Security Chain?" *Security Affairs*, 3 October 2012, http://securityaffairs.co/wordpress/9076/social-networks/why-humans-could-be-the-weakest-link-in-cyber-security-chain.html (accessed 18 November 2013).

Cyber-crime represents one of the fastest-growing areas of criminality; unique in that it is exclusively taking place in the cyber realm.[22] If the attacker is driven by monetary gain, destruction of property, or espionage, then a crime has been committed. Cyber crime ranges from simply penetrating a system and examining it for the challenge, thrill, or interest to entering a system for revenge, to steal information, cause embarrassment, extort money, or cause deliberate localized harm to computers or damage to larger critical infrastructures. Across the whole range of criminal cyber attacks, three categories can be delineated: cyber vandalism, cyber crime, and data theft. The realm for the resolution of these attacks normally lies in law enforcement, judicial systems, and legislatures.[23] If a terrorist group were to launch a cyber attack to cause harm, such an act fits within the definition of a cyber crime. The primary difference between a cyber attack to commit a crime or to commit terror is intent of the attacker. It is possible for actions fitting both definitions to overlap.[24] An example of a cyber-criminal organization is the Russian Business Network. Originally registered as an Internet provider in St. Petersburg, the founders soon discovered that it was more profitable to host illegitimate activities and started hiring its services to criminals. They operate as a platform, specializing in personal identity theft and generate profits of approximately $150 million a year.[25]

---

[22]Europol, Threat Assessment (Abridged), *Internet Facilitated Organised Crime (iOCTA*), (The Hague: Europol, 2011), https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf (accessed 18 November 2013).

[23]Fred Schreier, "On Cyberwarfare," DCAF Horizon 2015 Working Paper 7 (2012): 8, http://www.dcaf.ch/Publications/On-Cyberwarfare (accessed 18 November 2013).

[24]Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* CSR Report for Congress (Washington, DC: Congressional Research Office, 29 January 2008), 4, http://www.fas.org/sgp/crs/terror/RL32114.pdf (accessed 18 November 2013).

[25]David Bizeul, *Russian Business Network Study*, 20 November 2007, http://www.bizeul.org/files/RBN_study.pdf (accessed 18 November 2013).

Hacktivism is the act of breaking into a computer system for mainly politically or socially motivated purposes. Therefore, hacking and activism combine. Hacktivists use the same tools and techniques as a hacker, except that profit and data theft or severe damages are not important to hactivists.[26] A prominent hacktivist group is Anonymous; an internationally operating network of activists, which is decentralized without leadership. This group is a typical consortium of people who likes the apparent anonymity of the Internet to ensure a safe embarrassment of normally high-ranking societal authorities such as governments, public organizations, or economic institutions. They fight against apparent injustices in the modern world such as stock markets, banks, economic entities, or governments.[27] While most view such activities as criminal, others assess organizations like Anonymous as terrorists and potential virtual warfighters.[28] These studies are not helpful for a contextual assessment of cyber threats and hamper efficient and appropriate countermeasures.

Cyber-espionage is similar to cyber-crime. Espionage is defined as the practice of spying or using spies to obtain information about the plans, and activities especially of a foreign government or a competing company.[29] This is a twofold definition because it addressed two different entities: states and privates companies. Therefore, it is difficult to differentiate between an attack against a state and against private interests. The cyber realm provides an exceptional environment for espionage because it provides foreign collectors with relative anonymity,

---

[26]Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf (accessed 12 February 2014).

[27]Parmy Olson, *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency* (London: Random House UK, 2013), 24-53.

[28]Pierluigi Paganinip, "Hacktivism: Means and Motivations … What Else?" *Information Security Institute,* 2 October 2013, http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/ (accessed 12 February 2014).

[29]Merriam Webster Dictionary, s. v. "Espionage," http://www.merriam-webster (accessed 10 February 2014).

facilitates the transfer of a vast amount of information, and makes it more difficult for victims and governments to assign blame by masking geographic locations.[30] It is considered theft of commercial intellectual property and proprietary information, data with significant economic value, or the theft of government sensitive and classified information. These acts are defined by almost all nations as criminal acts first and espionage second.[31]

Companies and governments regularly face attempts by others to gain unauthorized access to their data and information technology systems through the Internet. One example of this is an unauthorized user masquerading as an authorized user or through the surreptitious introduction of malicious software.[32] Cyber espionage, particularly when targeting commercial intellectual property, potentially risks undermining a national economy. Many countries use espionage to spur rapid economic growth based on advanced technology, targeting science, and technology initiatives of other nations.[33] Because ICT forms the backbone of nearly every other technology used in both civilian and military applications today, it has become one of the primary espionage targets. Of course, military and civilian dual-use technologies will remain of interest to foreign collectors. This is especially true of advanced manufacturing technologies that can boost industrial competitiveness.[34] Accurate assessment of the monetary value of losses in technology and information is difficult, but it is reasonable to say that cyber espionage shifts the terms of

---

[30]US Office of the National Counterintelligence Executive, "Foreign Spies Stealing Us Economic Secrets in Cyberspace," Report to Congress On Foreign Economic Collection and Industrial Espionage, 2009-2011," http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (accessed 11 February 2014).

[31]Klimburg, *National Cyber Security Framework Manual*, 16.

[32]Joseph S. Nye and Brent Scowcroft, *Securing Cyberspace: A New Domain for National Security*, ed. R. Nicholas Burns and Jonathon Price (Washington, DC: Aspen Institute, 2012), 145-57.

[33]Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf (accessed 12 February 2014), 51-58.

[34]Klimburg, *National Cyber Security Framework Manual*, 16-17.

engagement in favor of foreign competitors. Illustrated by the recent leaks of classified information regarding whistleblower incidents, intelligence agencies are now beginning to understand digital espionage and the proper role of human informants in a digitized threat environment.[35]

Finally, the term cyber warfare is both ambiguous and controversial because there is no official or generally accepted definition. Cyber warfare has a useful academic purpose because it focuses thinking on interstate conflict within the realm of cyber. Various official documents view cyber warfare as military-type Inform and Influence activities. More than thirty countries define cyber warfare and each differs considerably in definition, meaning, importance, and possible counter measures.[36] Generally, cyber warfare involves actions by a nation-state or international organizations to attack to damage another nation´s cyber security means.[37] When nations begin to discuss cyber warfare they need to clarify what they mean. Examples of significant differences in meanings are Germany and the United States. Germany defines a cyber attack as an IT attack in the cyber realm directed against one or several other IT systems and aimed at damaging IT security—confidentiality, integrity and availability—which may all or individually be compromised.[38] The United States defines Computer Network Attack (CNA) as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident

---

[35]Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence," *Foreign Affairs* (November/December 2013): 1, http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace (accessed 4 February 2014).

[36]Klimburg, *National Cyber Security Framework Manual*, 17-25.

[37]Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 117-158.

[38]Federal Ministry of Interior, "Cyber Security Strategy For," http://www.cio.bund.de, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (accessed 11 February 2014).

in computers and computer networks, or the computers and networks themselves."[39] The US definition does not include attacks on confidentiality (i.e. through a 'probe' or espionage), as a cyber attack while, according to the German definition, there is no difference between a probe and a cyber-attack.

Regarding the definition and the different points of view, it is also difficult to distinguish between acts of war and criminal acts. For example, it is natural for the military to be ambiguous as to whether an attack is considered a use of force (as defined by the Law of Armed Conflict), whereas the law enforcement community (police and prosecutors) are more likely to describe an attack as a crime. In general, there is an agreement that cyber activities can be a legitimate military activity, but there is no global agreement on the rules that should apply. There is a very fine line between breaking into a computer network in order to spy and breaking into a computer network to conduct an attack. Whereas crime and warfare are clearly distinguishable, especially in case of different motivations, warfare and espionage possess common intersections.

Whether cyber warfare is a new kind of warfare or not is a widely discussed and controversial topic. The debate on cyber warfare is prone to speculation. Some proponents think that cyber warfare will eventually replace kinetic war.[40] More frequently, cyber warfare is presented as a new kind of fighting that is cheaper, cleaner, with little or no bloodshed, and less risky for an attacker than other forms of armed conflict. For a small nation with limited resources, this seems to make cyber warfare attractive.[41] This raises the question of what is the difference

---

[39]US Defense Department, Joint Publication (JP) 3-13, *Information Operation*, 27 November 2012, "http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed 5 February 2014).

[40]Andrew Krepinevich, "Cyber Warfare: a 'nuclear option'?" www.csbaonline.org, http://www.csbaonline.org/wp-content/uploads/2012/08/CSBA_Cyber_Warfare_For_Web_1.pdf. (accessed 5 February 2014).

[41]James A. Lewis and Katrina Timlin, "Cybersecurity and Cyberwarfare," http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-

between war and warfare. To answer this question, this study follows Carl von Clausewitz and his widely accepted definition of war, "[e]ach tries through physical force to compel the other to do his will; his *immediate* aim is to *throw* his opponent in order to make him incapable of further resistance. Force—that is, physical force, for moral force has no existence save as expressed in the state and the law—is thus the *means* of war; to impose our will on the enemy is its *object*."[42] In response to proponents of cyber warfare, Clausewitz would likely counter: "If one side uses force without compunction, undeterred by the bloodshed it involves, while the other side refrains, the first will gain the upper hand."[43] In this view, what is known currently as cyber war presents risk, politically and strategically, but is cyber misunderstood if it is included in the phenomenon of war? Clausewitz makes a determination between war and warfare, where current national security policy mistakenly does not. It is questionable that this risk can be mitigated or accepted where this endangers an entire national security policy.

As described, each single form of malicious cyber activity has inherent potentials to attack critical infrastructure. A cyber-doom scenario may demonstrate vulnerabilities, challenges for national security strategies and private business entities, which are highly important, and a matter of deep concern. This concern is especially important if private business companies operating critical infrastructure with national importance. Cyber-doom scenarios are hypothetical situations about prospective impacts of a cyber attack and are meant to serve as cautionary tales that focus the attention of policy makers, media, and the public on the issue of cyber security. These stories typically follow a set pattern involving a cyber attack disrupting or destroying critical infrastructure. Examples of cyber-doom scenarios includes: attacks against the electrical

---

assessment-of-national-doctrine-and-organization-380.pdf (accessed 5 February 2014). Thirty-three states with major activities, and thirty-six states with minor activities in cyber development.

[42]Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1989), 75.

[43]Ibid., 75-76.

grid causing mass blackouts, attacks against the financial system causing economic loss or complete economic collapse, attacks against the transportation system cause plane and train crashes, attacks against dams cause floodgates to open, or attacks against nuclear power plants causing meltdowns.[44]

One of the most controversial aspects of cyber attacks on national critical infrastructure is a possible attack on power grids and its critical equipment (e.g. generators, turbines, transformers). A simulated attack sponsored by the DHS, named the Aurora generator test conducted at Idaho National Labs, took place in March 2007. An electric generation turbine spins widely out of control when the generator was remotely taken over by computer hackers, demonstrating a vulnerability of the US critical infrastructure.[45] Even the Stuxnet worm, a far more specialized and sophisticated designed malware to attack Iran's nuclear capability in 2010[46] demonstrated a thoughtful example for cyber-physical attacks against critical infrastructure.[47] Assessing such attacks as an operation by virtual weapons, the fallacy becomes true that attacks have something to do with offense. Some assert that cyber offense has an advantage over cyber

---

[44]Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* (New York: Routledge, 2007), 2, http://www.academia.edu/462492/Cyber Security_and_Threat_Politics_US_Efforts_to_Secure_the_Information_Age (accessed 19 November 2013).

[45]Robert Lemos, "DHS video shows potential impact of cyberattack," http://www.securityfocus.com, http://www.securityfocus.com/brief/597 (accessed 21 November 2013).

[46]As one of the first, Ralph Langner, a computer expert, identified and encoded Stuxnet. See: Ralph Langner, "To Kill a Centrifuge-a technical analysis of what Stuxnet's creators Tried to achieve," http://www.langner.com, http://www.langner.com/en/wp-content/uploads/2013/ 11/To-kill-a-centrifuge.pdf (accessed 11 February 2014).

[47]Especially in reaction of the Aurora test see: Clay Wilson, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, CRS Report for Congress (29 January 2008): page nr., http://www.fas.org/sgp/crs/terror/RL32114.pdf (accessed 21 November 2013).

defense.[48] While some debate this is true in technical terms, in the domain of industrial control system security, it certainly does apply in a political context. Cyber offense is well funded and implemented within a military chain of command. Cyber protection is not the same as cyber defense. However, government and some experts expect cyber protection of critical national infrastructure be voluntary by a dispersed private sector that feels little desire to address matters of national security.

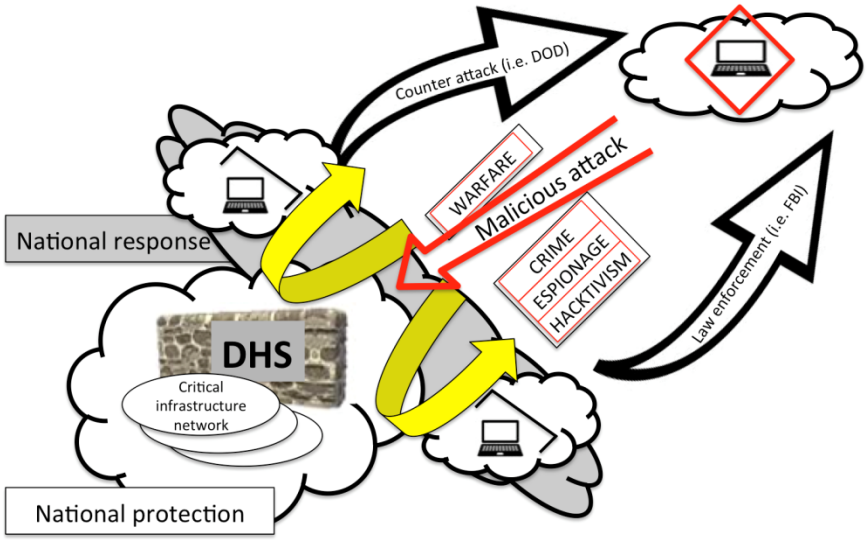

Figure 3. The Differences Between Protection and Defense in the Realm of Cyber Security

Source: Created by author.

The last two segments in this section are closer examinations of two important concepts: the distinction of protection and defense in the realm of cyber security and the challenge of the attribution of cyber attacks as a precondition to formulate a response through the appropriate

[48]David T. Fahrenkrug, *Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy*, http://www.ccdcoe.org/publications/2012 proceedings/ 3_4_Fahrenkrug_AnIntegratedDefensiveStrategy.pdf (accessed 5 February2014).

entity (protection agency vs. defense agencies). Figure 3 illustrates the arenas of responsibilities in concert with proper responses according to power sharing principles in the case of cyber attacks on critical infrastructure networks. If a malicious attack occurs, the analysis of the attribution factor (source of the attack) is key. The primary responsibility belongs to the protection authority, whose focus is the restoration of functionality of attacked critical infrastructure networks. The distinction of the source of attack is necessary for the next step, the response. Whether a reaction is military or law enforcement by nature depends on the motivation from the attacker´s perspective. Military counter attacks by the DOD are appropriate in case of warfare-type attacks, and law enforcement activities (e.g. FBI) are a better solution for security cooperation (e.g. with other countries). Overall, protection is passive, being solely responsible for security without any possible response measures. In concert with instruments of response, the realm of security is much more efficient in case of counter measures, which happen outside the arena of protection, nested in the arena of comprehensive cyber strategies with multiple synchronized actors (DHS, DOD, US law enforcement agencies). If-then principles, counter activities, and active by nature are the basis of defense. In case of possible military or civil responses, the term defense has its own shade of meaning, viewed as a political and strategic phrase.

The fact remains that the anonymity continues to reduce the probability of detection and discovery of the origin of an attack, thus making attribution a permanent problem. Attackers can route attacks through countries in which the victim's government has poor diplomatic relations or no law enforcement cooperation. Even successful investigations often lead only to another hacked computer. Thus, states and governments still face the prospect of losing a cyber conflict without ever knowing the identity of their adversary. Hence, responses limited to the level of the nation-state are inadequate. International cooperation is one key to reducing cyber security risks. Coordinated international activity, with the associated problems of reaching agreement and then

acting in concert, is a necessity. The international community can only identify attackers through close international cooperation. Moreover, vulnerabilities can be discovered and exploited through such cooperation.[49] Even the military emphasizes the requirement of an international collaborative effort. Activities in the cyber realm are international by nature. Besides this military understanding, endorsed at the Lisbon NATO summit in November 2010, an approach should not be a military-only or even a military-centric strategy. It cuts across the portfolio of a variety of actors.[50] The Internet is not completely anonymous, but digital forensics takes time to examine attacks and provide options for potential counter activities. Time, however, is often the critical factor in appropriate counter procedures. An international collaborative effort may help to mitigate the critical time factor.

This section illustrates the large-scale arena of the cyber realm, and the different kind of activities resulting in cyber threats. In particular, the risks to critical infrastructure sector originate from two different areas: the risk of manipulated ICT systems and the risk of attacks by the four different types of cyber threats (crime, hacker, espionage, and warfare). Some other significant challenges (i.e. cyber as a war) are sketched out in this section. Those will be intensively examined in the next section. Two conclusions are drawn from the discussion in this section: first, the threats are real and multilayered and second, not every cyber attack can be assigned to cyber warfare activities, no matter how severe the attack might be. In this respect, it is more important to analyze the source of the attacks and not the fact of the attacks. The four different main groups of cyber attacks are impelled by different motivations, and only one (the warfare group) should

---

[49]Kamlesh Bajaj, *The Cybersecurity Agenda: Mobilizing for International Action* (New York: East West Institute, 2010), 5-9, http://www.ewi.info/sites/default/files/ideas-files/Bajaj_Web.pdf (accessed 9 March 2014).

[50]Stéphan Abrial, "NATO Builds Its Cyberdefenses," *New York Times*, 27 February 2011, http://www.nytimes.com/2011/02/28/opinion/28iht-edabrial28.html?_r=0 (accessed 9 March 2014).

generate consideration of a military response. This enables a principal distinction between protection (that means the analysis of vulnerabilities, which can be protected) and defense (the analysis of risks, which are both protected but assailable). This difference is relevant in case of the appropriate assignment of response measures by the correct means (i.e. homeland protection vs. homeland defense). An analysis of critical infrastructure and the potential conflicts of interests between public and private sectors is the main issue of the next section.

CYBER EFFECTS ON CRITICAL INFRASTRUCTURE

The purpose of this section is twofold. The first part analyzes a possible new threat scenario from a political perspective in the event of cyber attacks on the United States' critical infrastructure. This analysis focuses on existing general vulnerabilities rather than specific cyber-doom-scenarios. One major argument will be that large-scale cyber attacks are possible any time even without a simultaneously conducted armed conflict against the American homeland. The second part is focused on possible approaches of solutions. Starting from the perspective of a permanent threat to the homeland and its political implications, the analysis highlights two areas: domestic mechanisms and military mechanisms, each possessing a general approach to cope with cyber attacks. The final segment of this section will represent both mechanisms as a dilemma.

President Obama declared critical infrastructure was the backbone of national and economic security, underlining its importance.[51] Critical infrastructure is the framework of interdependent networks and systems comprising identifiable industries and institutions including people and procedures. Furthermore, infrastructure distributes capabilities that provide a reliable flow of products and services essential to the defense and economic security of a state, the smooth functioning of government at all levels, and society as a whole. According to the DHS,

[51]White House, "Presidential Proclamation—Critical Infrastructure Security and Resilience Month, 2013," http://www.whitehouse.gov/the-press-office/2013/10/31/presidential-proclamation-critical-infrastructure-security-and-resilienc (accessed 5 February 2014).

infrastructure includes physical, cyber, and human elements. Critical infrastructure are assets, systems, and networks, whether physical or virtual, so vital to a state that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters.[52]

How can risk associated with an attack on critical infrastructure be estimated? There is no historical answer because a successful complex attack on critical infrastructure has yet to occur in America. Cyber hype takes potential vulnerabilities, speculates on the potential risk, and is an overestimation of the actual risk. A more precise question is whether an attack is possible only under specific circumstances. One example is the energy sector. The US electrical system is composed of several thousand public and private utilities organized into ten large regional grids. There is a substantial degree of interconnection within these grids and computer networks play an important role in managing grid operation and the production of electrical power. However, the grids themselves suffer from the consequences of underinvestment and deregulation. Newer industrial control systems use commercial computer operating systems and Internet protocols (IP), because they are cheaper and easier to use. However, the new technologies replace older control systems that used specialized proprietary software and dedicated networks, which is difficult for hackers to access and exploit. The move to commercial software and IP increases vulnerability.[53] Contextually, vulnerabilities are identified weak points, which need protection. One should analyze not only risk with respect to the identified general vulnerabilities but also in terms of specific vulnerabilities. It is possible for there to be an identified risk without a specific

---

[52]Department of Homeland Security, *National Infrastructure Protection Plan* (Washington, DC: Government Printing Office, 2009) http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed 5 February 2014), 109.

[53]James A. Lewis, "Cybersecurity and Critical Infrastructure Protection," Center for Strategic and International Studies, entry posted January 2006, http://csis.org/files/media/csis/pubs/0601_cscip_preliminary.pdf (accessed 5 February 2014).

vulnerability. Impact, vulnerability, and weakness are the basis for risk. It is possible to have a national asset that is so attractive to attack that it does not matter if it is weak or not—it will be attacked. It follows that there are vulnerable areas that have no protection, but will have no impact if attacked. Vulnerability is not the same as risk, however the two are often used interchangeably with regards to specific protection of critical infrastructure. Defense, protection, vulnerability, and risks have become an abstract and inscrutable conglomerate of meanings.

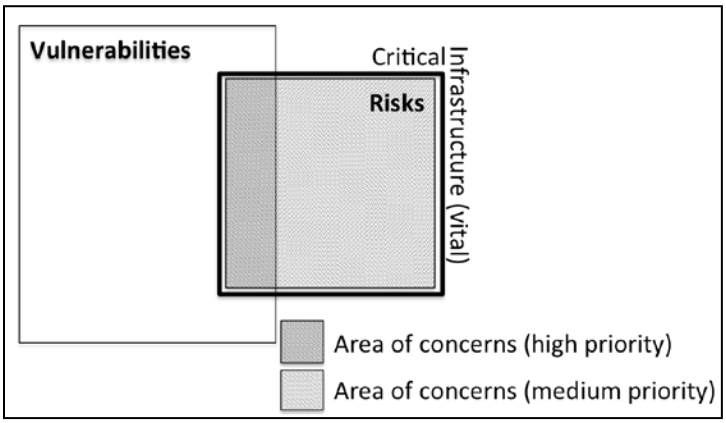

Figure 4. The Differences Between Vulnerabilities and Risks in the Realm of Cyber Security

Source: Created by author.

The 2013 *Presidential Policy Directive for Critical Infrastructure Security and Resilience* served as a new prelude for coordinated efforts under lead of federal government agencies. This endeavor encompasses federal, state, local, tribal, and territorial (SLTT) entities, and public and private owners and operators of critical infrastructure. The DHS has a primary role in responsibility of maintaining the unity of effort. In the paper, the Department of Defense (DOD) was only mentioned four times, each time in a supporting role. The document identifies sixteen designated critical infrastructure sectors and designates associated Federal Sector-Specific-

Agencies (SSAs).[54] In an exact examination of critical infrastructure components, it appears that private owners or operators are responsible for approximately eighty-five percent of US key infrastructures.[55] The private sector is an increasingly important factor of the new security issues associated with homeland security. This demonstrates that national security and homeland security differs in its shared responsibility and cannot be met by the federal government alone. This fact illustrates the importance of a whole-of-nation approach rather than the whole-of-government approach.

The Dot-Com Challenge and Cyber Hype

The former Secretary of Defense, Leon E. Panetta, viewed the cyber realm as a new frontier consisting of "…[a] new terrain for warfare where adversaries can seek to do harm to our country, our economy and our citizens."[56] He used the term cyber Pearl Harbor as a synonym for a destructive scenario of several cyber attacks on critical infrastructure in the country.[57] Why is a cyber Pearl Harbor possible and what does that mean for the current perception of war? Two different perspectives can approach the first part of the question. The *dot-com challenge* is a general assessment about the risks of private and public operating critical infrastructure issues.

---

[54]White House "Presidential Proclamation—Critical Infrastructure Security and Resilience Month, 2013," http://www.whitehouse.gov/the-press-office/2013/10/31/presidential-proclamation-critical-infrastructure-security-and-resilienc (accessed 5 February 2014). Chemical sector, Commercial Facilities, Communications sector, Critical Manufacturing sector, Dams sector, Defense Industrial Base sector, Emergency Services sector, Energy sector, Financial Services sector, Food and Agriculture sector, Government Facilities sector, Healthcare and Public Health sector, Information Technology sector, Nuclear Reactors, Materials, and Waste sector, Transportation Systems sector, Water and Wastewater Systems sector.

[55]Sue Eckert, "Protecting Critical Infrastructure: The Role of the Private Sector," http://www.ridgway.pitt.edu, http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf (accessed 11 February 2014).

[56]Secretary of Defense Leon E. Panetta "Defending the nation from cyber attack" *Business Executives for National Security*, 11 October 2012, http://www.bens.org/document.doc?id=188 (accessed 5 February 2014).

[57]Ibid.

The second perspective is based on so-called cyber hype; the mainly economic approach to articulate an overwhelming cyber threat into thinking that because of its potential to be both ubiquitous and extremely harmful. Using the example of the United States, the last part will show a changing perception of war in case of the identified vulnerabilities and the concurrent political discussions to cope with the challenge.

While a variety of government-industry initiatives evolved to address critical infrastructure protection issues, several serious challenges remain that are likely to hinder effective partnerships between the government and private entities. The Information Sharing and Analysis Centers (ISACs), which are the primary vehicles to address infrastructure protection concerns, were initiated after *Presidential Decision Directive 63* (PDD-63) in 1998. The main purpose of this directive was to specifically focus on coordination and organization of information sharing among all related actors and owners of critical infrastructure within the federal government. However, this organization is struggling to fulfill its purpose.[58] The biggest problem is the lack of interagency trust, especially between competing private industries. In addition, increasing mistrust between private industry enterprises and federal security agencies reveals challenges for an efficient protection.[59] The gap between the lip service, its idealistic point of views of creating efficient public-private partnerships to address security issues in the cyber realm, and the reality of actions to support the issues is significant and endanger the entire whole-of-nation approach.

Within the relevant academic discourse are three schools of thought. The most important distinguishing criterion is the perception of cyber threats as a warfare element in its nature. The

---

[58]Information Sharing and Analysis Centers (ISAC), "The Role of Information Sharing and Analysis Centers (ISACs) in Private/public Sector Critical Infrastructure Protection," http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf (accessed 5 February 2014).

[59]DER SPIEGEL, "NSA spying scandal," http://www.spiegel.de/international/topic/nsa_spying_scandal/ (accessed 5 February 2014).

first group does not see the logic of the potential for cyber attacks without involving also high-intensity physical conflicts in the absence of evidence that real damage can be achieved through the cyber realm alone. This group does not see any nation-state capable of using a combination of cyber attacks and combat operations against the American homeland. The second group believes in the likelihood of a cyber attack without an accompanying act of physical violence. Members of this faction are either involved experts or a result of the popular main stream of cyber hype. The third group, while seemingly extreme, should be taken very seriously as some among this group can wield significant influence. This third group also believes in separated cyber attacks on critical infrastructure. They argue for a comprehensive response, not only virtually, but also physically. Furthermore, this superficially economic focused approach actually argues that an attack on private industry, which is providing critical infrastructure services, is an attack on the state in a broader sense.[60] This thinking mixes every single form of cyber threats (crime, hacktivism, espionage, and warfare) to one huge threat scenario.

One of the challenges to predicting possible realistic cyber attack scenarios is profound impact the proliferation of cyber hype scenarios has on policy making. In many cases those now inflating the scope and probability of cyber threats are those who will benefit from increased regulation and more government spending on information security. Cyber security is a large and growing industry.[61] The US government is expected to spend $10.5 billion per year on information security by 2015 and analysts have estimated the worldwide market to be as much as

---

[60]Mike Rogers, "US businesses are in an unfair fight against cyber threats," My opinions, entry posted 23 October 2013, http://www.washingtonpost.com/opinions/mike-rogers-us-businesses-are-in-an-unfair-fight-against-cyberthreats/2013/10/22/5a5167b8-3b32-11e3-b6a9-da62c264f40e_story.html (accessed 5 February 2014).

[61]Marjorie Censer and Tom Temin, "The Cybersecurity Boom," *Washington Post*, 10 May 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/05/07/AR2010050704503.html (accessed 19 November 2013).

$140 billion per year.[62] The DOD has also said it is seeking more than $3.2 billion in cyber security funding for 2012.[63] In addition to traditional information security providers like MacAfee, Symantec, and Checkpoint, defense contractors and consulting firms have recognized lucrative opportunities in cyber security.[64] To weather probable cuts on traditional defense spending, and to take advantage of the growing market, these firms have positioned themselves to compete with information security firms for government contracts.[65] Lockheed Martin, Boeing, L-3 Communications, SAIC, and BAE Systems have all launched cyber security business divisions in recent years.[66] Other traditional defense contractors, like Northrop Grumman, Raytheon, and ManTech International, have also invested in information security products and services.[67] Such investments appear to have positioned defense firms well. In 2009, the top ten information technology federal contractors included Lockheed Martin, Boeing, Northrop Grumman, General Dynamics, Raytheon, SAIC, L-3 Communications, and Booz Allen

---

[62]Homeland Security News Wire, "US Cybersecurity Spending to Rise," http://www.homelandsecuritynewswire.com, http://www.homelandsecuritynewswire.com/us-cybersecurity-spending-rise (accessed 11 February 2014).

[63]Nextgov, "Cyber Spending at Defense," http://www.nextgov.com/cybersecurity/2011/03/cyber-spending-at-defense/48790/ (accessed 11 February 2014).

[64]Aaron Ricdela, "Symantec, Mcafee, Checkpoint Await Spending Surge," *Business Week* (18 January 2010), entry posted 18 January 2010, http://www.businessweek.com/technology/content/jan2010/tc20100115_453540.htm (accessed 19 November 2013).

[65]August Cole and Siobhan Gorman, "Defense Firms Pursue Cyber-Security Work," *Wall Street Journal*, 18 March 2013, http://online.wsj.com/news/articles/SB123733224282463205 (accessed 19 November 2013).

[66]Marjorie Censer and Tom Temin, "The Cybersecurity Boom," *Washington Post*, 10 May 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/05/07/AR2010050704503.html (accessed 19 November 2013).

[67]Homeland Security News Wire, "US Cybersecurity Spending to Rise," http://www.homelandsecuritynewswire.com/us-cybersecurity-spending-rise (accessed 11 February 2014).

Hamilton.[68] Traditional IT firms also see more opportunities to profit from cyber security business in both the public and private sectors.[69] Earlier in 2011, a software security company executive noted a very large rise in interest in spending on computer security by the government. Some companies from diverse industries have also combined forces in the cyber security buildup. In 2009, a combination of defense, security, and technology companies, including Lockheed, McAfee, Symantec, Cisco, Dell, Hewlett-Packard, Intel, Juniper Networks, and Microsoft, formed a cyber security technology alliance to study threats and create solutions.[70] IT lobbyists too have looked forward to cyber security budget increases, to the dismay of at least one executive at a small tech firm, who claimed, "[M]oney gets spent on the vendors who spend millions lobbying Congress."[71] There are serious real online threats, and security firms, government agencies, the military, and private companies clearly must invest to protect against such threats. However, as with the Cold War bomber and missile gap frenzies, we must be wary of stake holding parties who may be prone to exaggerating threats, leading to unjustified and superfluous defense spending in the name of national security.

Based on these two different perspectives, determining cyber threats leads to a discussion about the perception of war in the United States, which is a dominate discourse and creates many problems to capsulate the real challenge. Besides, this consideration also applies to other western European states, which do not assume symmetric and physical attack through an armed conflict to

---

[68]Tom Barry, "Synergy in Security: The Rise of the National Security Complex," *Dollars and Sense* (April 2010), http://www.dollarsandsense.org.archives/2010/0310barry.html (accessed 19 November 2013).

[69]Aaron Ricdela, "Symantec, Mcafee, Checkpoint Await Spending Surge."

[70]Dan Lohrmann, *New Cybersecurity Technology Alliance Points the Way*, 13 November 2009, http://www.govtech.com/blogs/lohrmann-on-cybersecurity/New-Cyber-Security-Technology.html (accessed 19 November 2013).

[71]John Leyden, "US and UK Gov Cyber Defences = Big Boys' Trough-Slurp," http://www.theregister.co.uk, 22 October 2010, http://www.theregister.co.uk/2010/10/22/firewall_guru_interview/ (accessed 19 November 2013).

their own homeland in the near future.[72] The problem in the entire discussion is twofold. The first issue is the widely discussed and misinterpreted analogy of overwhelming cyber threats using a metaphor of war. The second issue is an inappropriate mixing of politico-military terms, in essence, failing to distinguish between protection and defense at the political-strategic level. This combination of thinking brings the military into a new sphere of responsibility outside the legal framework of a democratic nation.

Cyberwar?

Activities in the cyber realm depend on the different motivations of actors, who conduct those activities. The differences between crime, hacktivism, espionage, and warfare have already been discussed in the first section. However, none of these activities meets the character and the definition of war. Cyber warfare measures would simply reflect the nature of warfare in conjunction with traditional warfare activities. The use of cyber activities in the Russo-Georgia-War in 2008 is an illustrative example.[73] According to Clausewitz's theory, war is a kind of a large-scale duel by the use of physical force to compel the will upon the enemy. This implies several characteristics of war. War has to be violent or potentially violent and its instruments (physical force) must have some kind of political goals and intentions. [74] Even the law of war, codified in the United Nations Charter, covers the issue of *Jus ad bellum* and *jus in Bello*, which constitute armed conflicts by use of forces.[75] There are no international agreements on the proper

---

[72]Klimburg, *National Cyber Security Framework Manual*, 23-25.

[73]Timothy L. Thomas, *Recasting the Russian Star. Russia Forges Tradition and Technology through Toughness* (Fort Leavenworth, KS: Foreign Military Studies Office (FMSO), 2011), 313-63.

[74]Clausewitz, *On War*, 75.

[75]Chapter VII: Actions with respect to threats to the peace, breaches of the peace, and acts of aggression; Article 41, In: The United Nations, "Charter of the United Nations and Statute of the International Court of Justice," https://treaties.un.org, https://treaties.un.org/doc/publication/ctc/uncharter.pdf (accessed 11 February 2014).

conventions regarding cyber within a larger context of war. This has created an increased tendency to take cyber as a new perspective of war outside prevailing norms and definitions.[76] The fear of a theoretical overwhelming cyber attack on the homeland is influencing discussions away from established rules and meaning of terms.

The misuse of terms in accordance with misleading metaphors created an academic environment of mainly two fractions: those who differentiate between cyber war and cyber warfare and those who do not. A metaphor is useful to understand contexts better and to serve as an opportunity to open new conceptual ideas and discussions.[77] Beside the fact that no cyber attack has happened which meets the criteria of war, cyber war continues to be a subject of intense fascination.

Based on the demonstrated problems of definitions and terms and their use in another context, a second issue arises; the militarization of political-strategic level. The inappropriate mixing of politico-military terms, particular in the distinction of protection and defense on the political-strategic level, resulted in an unclear demarcation between internal and external security and subsequently in a conceptual conflicts of responsibility between two USG departments: DHS (protection) and the DOD (defense). It is increasingly difficult to differentiate between protection and defense of the homeland. However, in case of no differentiation this approach militarizes protection and provides new mission sets for the military. How can the Armed Forces defend a country without protection? From a military point of view, the problem is imminent and restrictive. From a state perspective, the problem is unsolved. Although the working solution may

---

[76]Following, there are two examples of a misleading discussion about cyber war and its relevance for military and civil developments. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 118-37; Martin C. Libicki, *Crisis and Escalation in Cyberspace* (Santa Monica, CA: RAND Corporation, 2012), 123-45.

[77]George F. Lakoff and Mark Johnson, "Metaphors We Live By," 124-134, http://pages.vassar.edu, http://pages.vassar.edu/theories-of-the-novel/files/2013/04/Metaphors-We-Live-By.pdf (accessed 11 February 2014).

exceed the legal framework, it is permissible as an accepted interim solution because of either a lack of domestic means, or an inability to take the time to coordinate an efficient plan for action within the correct legal framework; the ends justifying the means should be an unsatisfactory situation for the military.

This segment shows how possible cyber attacks on the American critical infrastructure create a hodgepodge of different perceptions of cyber. That leads into diverse definitions of war, intensified by the cyber hype, (pseudo-) academic discourses, and practical solutions away the legal framework stressed by the policy. Ultimately, the unsolved challenge of an adequate response illustrates a complicated dilemma. On the one hand, cyber attacks do not recognize different domestic and external responsibilities in a state, which makes it complicated to identify the correct acting agency. On the other hand, the use of military capabilities in domestic affairs regarding to cyber activities is a way from the constitutional approach and the military is referring to the terminology of war simply the wrong mean for the right purpose. The contradictory tendencies are unproductive and potentially dangerous.

The next part demonstrates the actual level of development of both the state and the military. Thus, the final analysis strengthens the main argument of this paper, that the military should take a back seat in cyber defense of the homeland. Each different consequence based on the various perspectives (military and governmental points of view) of cyber is in focus of this part. The main argument in this portion is that the different stages of development are also a result of the misperception of cyber threats and finally, who is responsible for it. The present government approach drives the military´s viewpoint of its role in the cyber realm.

The Military Approach

The DOD directs all services to treat the cyber realm as a domain similar to land, sea, air, and space. A comprehensive military approach was established with a strategy subsequently gaining advantages from its potential. Developed as an additional tool in support of combat

operations on an operational and tactical level, thinking about cyber is going far beyond that.[78] In the US military, there are two different organizations, which combine perfectly the entire spectrum of military defensive and offensive cyber operations. The National Security Agency (NSA) as a governmental organization under the DOD and the US Cyber Command, a sub-unified command and subordinate to the US Strategic Command. This section will demonstrate the different military capabilities of NSA and US Cyber Command in consideration of their role in a strategic and state-focused context. This analysis will answer a main portion of the question, why the military should not play a major role in a political and strategic way in coping the cyber threat of the United States. Special attention will be paid to the current considerations to reestablish organizational structures of NSA and US Cyber Command and the topical challenges of the NSA.

The beginning of the NSA goes back to World War I in 1917.[79] The organization was tasked with decoding, translation, and analyzing foreign intelligence and maintained its role through World War II.[80] In 1952, the agency was formally established. The NSA maintained and developed its key capability of signal intelligence (SIGINT), but 9/11 was a decisive turning point for the NSA for two reasons. The first was a tremendous extension of the legal framework. The war on terror, especially the Patriot Act, enables a larger spectrum of actions. The differences in the meaning between defense and protection has become more and more unclear, a main criterion to differentiate the purposes of the Department of Homeland defense and the

---

[78]Russell Fenton, "A combined arms approach to defending Army networks," http://www.dtic.mil/dtic/tr/fulltext/u2/a577086.pdf (accessed 5 February 2014), 20.

[79]George F. Howe, "The Early History of NSA," http://www.nsa.gov, http://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf (accessed 5 February 2014).

[80]Thomas L. Burns, "The Origins of the National Security Agency (1940-1952)," www.nsa.gov, http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf (accessed 5 February2014).

Department of Defense in interior and exterior affairs. Terrorism does not fit a traditional paradigm and cannot be fixed exclusively as an external or internal threat.

The second opportunity was the rising importance of the Internet in conjunction with its inherent problems for security issues. Internet communication and signal based communication (telephone) was not differentiable anymore and merged together in use and importance. Conversation is not only based on signal communication anymore. Therefore, the recently enlarged competencies in connection with the war on terror and the increased risk of the United States to be affected by cyber activities opens a new era of NSA. However, it presents new challenges for the NSA as well. The tapping and collection of telephone and internet communication, its content and metadata-based, from domestic sources and foreign origins makes the NSA to a very powerful military organization with a much broader spectrum of responsibility than originally designed. Generally, the NSA fulfills an almost perfect requirement of cyber defense.

The executive arm of the NSA is the US Cyber Command. This organization, which organizes the military´s cyber resources and synchronizes cyber operations, was established in 2009. Designed for an integral part of Information Operations (in conjunction with Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception, and Operations Security) in concert with specified supporting and related capabilities in the entire military spectrum,[81] US Cyber Command protects the DOD networks and provides capabilities for offensive cyber attacks.[82] The director of the NSA serves concurrently as the Commander of

[81]US Department of Defense, "Department of Defense Directive O-3600.01," www.fas.org, http://www.fas.org/irp/doddir/dod/info_ops.pdf (accessed 5 February 2014).

[82]US Strategic Command, "US Cyber Command," http://www.stratcom.mil, http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 5 February 2014).

US Cyber Command.[83] For reasons of secrecy, capabilities of US Cyber Command to conduct cyber activities cannot be discussed here. However, it can be presumed that the spectrum of responsibility and the area of interest are much broader than necessary for a military organization. There are two reasons for this assumption. First, the dual-hatted chief of both organizations, the NSA and US Cyber Command, enables effective information to flow between the two institutions without bureaucratic and structural obstacles. The situational picture in US Cyber Command is much better with this function than without. Second, the nature of cyber security, like the cyber threat environment, does not notice national boundaries and subsequently ignores the people`s legal rights and highlight the importance to separate the variety of power in a democratic state. However, incidents during the last year have been shown that the NSA is doing much more than military security agencies normally do.

Due to these facts, it is less important what the NSA is doing as a spy agency in foreign affairs rather how it impacts spying domestically. Nevertheless, the NSA is acting in a wide range of a legal framework designed by the policy. Originally, federal laws called Foreign Intelligence Surveillance Act (FISA) of 1978, which limit surveillance measures within the US by legal domestic authorities (which does not include the NSA), regulated the legal framework on US citizens or permanent residents. The 9/11-attacks and subsequently adapted legal frameworks (Patriot Act 2001, 2006) restructured the landscape of security agencies and provided a broad framework that has been expanded through interpretation. [84] The 2008 FISAAA (FISA

---

[83]US Department of Defense, Joint Publication (JP) 2-01, *Joint and National Intelligence Support to Military Operations* (5 January 2012), II-16, http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf (accessed 5 February 2014).

[84]US Government, Uniting and Strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001, Public Law 107–56—October 26, 2001 (Washington, DC: Government Printing Office, 2001); US Government, USA Patriot Act additional reauthorizing amendments act of 2006, Public Law 109–178—March 9, 2006 (Washington, DC: Government Printing Office, 2006).

Amendment Act) extended the competencies, inter alia, of the NSA.[85] This act enables NSA-activities to monitor US citizens, to see if they have something to do with foreign relations. For a globally acting country like the USA, this is not a limit for a military security agency anymore.

Growing cyber threats, in conjunction with misperceptions of cyber war spurred by cyber hype, obtains the relevance of unrestricted competencies. The resulting and controversially discussed public debate will result in modifications to the USG´s approach to cyber security in the future.[86] A report from the NATO Co–operative Cyber Defense Centre of Excellence (CCDCOE) concluded, "new approaches to traditional LOAC (law of armed conflict) principles need to be developed."[87] It advocated that the advent of new bloodless types of warfare required a definition of an attack not strictly connected with established meanings of death, injury, damage, and destruction.[88] There is evidence to suggest that US policy–makers and military leaders are also beginning to adopt this view.

In summary, the evolution of strategic-military capabilities is a significant response to growing cyber threats. US Cyber Command is mainly focused on cyber capabilities in accordance with international traditional warfare options. The NSA´s encroachment into domestic security matters represents a sharp deviation from the international focus they were originally designed for. Equipped with a wider legal framework, the NSA is acting externally and domestically. The

---

[85]US Congress, House, *The amend to the Foreign Intelligence Surveillance Act of 1978*, 110th Cong., H.R. 6304 (Washington, DC: Government Printing Office, 2008).

[86]US Department of Defense, "The Pentagon's New Cyber Strategy," http://www.defensenews.com/print/article/20110818/C4ISR02/108180316/The-Pentagon-s-new-cyber-strategy (accessed 11 February 2014). Deputy Defense Secretary William Lynn, 18 August 2011 "Establishing robust cyber defense no more militarizes cyberspace than having a Navy militarizes the ocean."

[87]Eneken Tikk, Kadri Kaska, and Liis Vihul, *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010), 101-5, http://www.ccdcoe.org/publications/books/legalconsiderations.pdf (accessed 4 February 2014).

[88]Ibid.

analysis of domestic capabilities other than NSA will show whether the domestic action of NSA, regarding cyber threats on critical infrastructure, is redundant to civil agencies or not.

Domestic Mechanism

Former Secretary of Homeland Security Michael Chertoff stated that the present cyber risk is shocking and unacceptable.[89] "Control systems" vulnerabilities threaten power plants and the critical infrastructure they support, from dams to hospitals … [and] threat is only going to get worse. Inaction is not an acceptable option."[90] The NSA warned hackers could have the ability to take down the entire US electrical grid within the next two years.[91] This concern echoes throughout the US administration, which initiated several cyber security strategies over the last years.[92]

In February 2013, President Obama issued an executive order outlining steps his administration will take to protect critical US infrastructure from cyber security threats. The order is a directive for a collaborative effort between the government and the private sector to reduce and mitigate cyber threats and risks to the US critical infrastructure. It encourages the

---

[89]Michael Chertoff, et al., "Letter to the Majority Leader Reid and Minority Leader McConnell," http://pdfserver.amlaw.com/cc/120119_ cyber_letter.pdf (accessed 11 February 2014).

[90]Ibid.

[91]Graham Smith, "Hacking Group Anonymous Shut Entire US Power Grid Head National Security Warns," *Daily Mail*, 22 February 2012, http://www.dailymail.co.uk/news/article-2104832/Hacking-group-Anonymous-shut-entire-U-S-power-grid-head-national-security-warns.html (accessed 4 February 2014).

[92]White House, "The National Security Strategy of the United States, 2006." http://georgewbush- whitehouse.archives.gov/nsc/nss/2006/ (accessed 5 February 2014); White House, "The National Security Strategy of the United States, 2010," http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed 5 February 2014); White House, "The National Strategy to Secure Cyberspace, 2003," http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed 5 February 2014); White House, "The Comprehensive National Cybersecurity Initiative, 2009," http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed 5 February 2014).

development of a process to rapidly share unclassified information with specified targets and a voluntary classified information-sharing program for eligible entities. The order also calls for the development of standards to identify critical infrastructure at the greatest risk. Operators and owners of identified critical infrastructure will be confidentially notified and may request reconsideration of this status. In addition, the order provides for the development of a voluntary cyber security framework outlining standards, methodologies, procedures, and processes to address cyber security risks while balancing policy, business, and technological concerns.[93]

A resulting national cyber-security-policy, designed to eliminate reasonably avoidable risks based on best practices, is one important way to align public and private goals. To manage a national cyber security policy effectively a single government office or agency leading the effort can help create clarity and minimize the many jurisdictional obstructions. The proper entity must have the authority to create and implement national policies through public and private critical infrastructure superintendence. This authority necessitates a broad cross-spectrum understanding of the cyber environment. It also requires a level of operational expertise to effectively collaborate with public and private critical infrastructure managers and stakeholders to implement ground-level strategy and oversee the standard-setting process. [94] This explains the need for a large agency with significant authority over every element of national cyber security, as well as the cost of creation and the political resistance to do so. This means the DHS.

---

[93]White House, "Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11737-1144 (19 February 2013)," https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity (accessed 4 February 2014).

[94]Committee on Homeland Security House of Representatives 112th Congress, "Examining the Homeland Security Impact of the Obama Administration´s Cyber Security Proposal," http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72253/pdf/CHRG-112hhrg72253.pdf (accessed 11 February 2014).

As demonstrated, the main responsibility for protection of critical infrastructure from cyber threats is the DHS. The National cyber security and Communications Integration Center (NCCIC) serves as the centralized institution where regarding issues are coordinated and integrated. Furthermore, the DHS is cooperating with other federal agencies and departments. Based on the *Presidential Decision Directive 63* (PDD-63) of 1998 in addition to the *Homeland Security Presidential Directive Seven* (Critical infrastructure identification, prioritization, and protection) responsibilities are clearly assigned, dividing the sixteen different critical infrastructure sectors into fields of actions. The DHS covers the majority of the sectors followed by other civil departments.

The Department of Defense, mainly responsible for the protection of defense industrial bases, plays a minor and subordinate role in this field.[95] Mainly designed around a whole-of-government approach, different branches and centers operationalize linkages to private organizations operating critical infrastructures. Analysis demonstrated that the linkages are not efficient enough. In case of this, the much better whole-of-nation-approach remains an ineffective solution to cope the situation. This raises the question of how the government is trying to close the gap of an effective foreign affairs defense through efficient military capabilities and not the existing private related domestic cooperation. In case of secrecy, assessments are based on assumption rather than facts. Currently, debates around NSA scandals contain a certain amount of clarity and a sphere of speculations. Some points relate to public-congressional debates revealing procedures of the NSA and other agencies by the government. On the other hand, transfers of competencies and shifts of legal authorizations are facts. DHS is cooperating with the NSA and

[95]Department of Homeland Security, "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection," http://www.dhs.gov/homeland-security-presidential-directive-7 (accessed 5 February 2014).

US Cyber Command in domestic affairs, clearly stated in a memorandum of agreement between the DHS and the DOD from 2010.[96]

It is important to distinguish between Homeland Security and Homeland Defense as separate instruments of national power. Homeland security is the concerted national effort to prevent attacks within the US with primary responsibility resting with the Department of Homeland Security. Homeland defense is defined as the military protection of US territory, the domestic population, and critical defense infrastructure against external threats and aggression. The DOD is primarily responsible for homeland defense. Following the 9/11 attacks, defense of the homeland was restored as a primary mission of the DOD.[97] This allows the deduction of a practiced displacement effect of the DHS by the DOD.

The military is becoming a major factor within the US domestic security architecture. Regardless of whether or not the military has the capacity to defend against cyber threats, the concern about DOD involvement into domestic affairs has significant political consequences for liberal democracy. The denying of existing differences between protection and defense from a military and political point of view is one reason for this argument. This manifests itself in controversially debated discourses in the public, on domestic political level, and regarding international relations. The military must actively participate in the discussion within the federal government on its current and projected cyber security role. The danger lies in allowing other agencies and actors to define the role for the DOD, which places the DOD in a position of unpreparedness and difficulty.

---

[96]Department of Homeland Security and the Department of Defense, "Memorandum of agreement between the regarding cyber security," 13 October 2010, http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed 5 February 2014).

[97]Steve Bowman, "Homeland Security: The Department of Defense's Role," www.fas.org, http://www.fas.org/man/crs/RL31615.pdf (accessed 5 February 2014).

As a result of this paper, the following main arguments are demonstrated: In the first part of the study, a specific analysis of cyber realm serves as an example of a general clarification of the high potential cyber threat. A particular focus was on the various kinds of protagonists as cyber attackers by their nature and motivation and the need to differentiate attacks in case of individual attributions (criminal, espionage, and hacktivist attack vs. warfare-type attacks). Furthermore, it is relevant to distinguish between protection and defense to take various forms of responses. The US security architecture includes different entities providing counter measures, which mainly divides between military and law enforcement agencies. An erroneously used effort by a specific mean may have severe political implications. Thus, a criminally motivated cyber attack on US critical infrastructure answered by US military means can cause the targeted country to view the counterattack as an act of war.

In the case of US critical infrastructure protection, there is a considerable difference between ambition and reality (how processes are supposed to be in contrast and how they actually are). This is particularly evident in contrast between postulated concepts (strategies and initiatives) and its effective implementations. The development of DHS´s displacement by the DOD in protecting measures is one example. This development has three reasons. First, the whole-of-nation-approach, the preferred effort, in US cyber security is not efficient enough. Due to partly supported cooperation from private operated critical infrastructure sector, the protection is not given. Second, cyber hype is an omnipresent fact, drawing an exaggerated picture about cyber threats. Finally, the second factor is influencing the third factor, which uses the cyber hype for war metaphors and military terminology. Thus, the military becomes a plausible means for domestic affairs.

CONCLUSION

Formally, the United States fulfilled the Clausewitzian requirement for war by placing defense first and offense second.[98] The peacetime US domestic-international security model offers a protection-defense-offense structure. The DHS provides the first line of protection and the military serves as the tool for defense and offense. However, regarding cyber security threat, the DOD has absorbed the role of the DHS through the broad and expansive actions of the NSA in domestic cyber security matters. The military and related agencies (i.e. NSA) are in the first line of defense of US soil and additionally tasked to protect against cyber threats to critical infrastructure. This transformed scope of responsibility is the result of institutional differences between protection (normally civil agency related tasks) and defense (military related tasks). The evolution of responsibilities is assessed as an adaptation in response of the growing threats of US critical infrastructure. The challenges to bring private enterprise into a governmental-led whole-of-nation-approach are the main reasons to expand competencies of governmental organizations (i.e. the military). Therefore, this policy prefers more the purpose than the sense or a the-end-justify-the-means-approach.

Behind this, the present effort has inherent and various problems, which may endanger the entire effect. First, the struggling whole-of-nation-approach is due to an existing mistrust between governmental and private entities. Overregulation of cyber security measures, enforced cooperation with governmental institutions. The required implementation of software and cyber backdoors for a better control of private industrial companies through security agencies is effective but not efficient for trust-building measures. These actions are more short-term oriented rather than to be mid and long-term solutions. Second, this approach endangers the public support finally operationalized by congressional pressure on the government. The fear about a militarized

[98]Clausewitz, *On War*, 357-359.

Internet, a loss of personal privacy, and ultimately Orwellian 1984 scenarios may have public pressure on congressional representatives. Often, congressional demands may focus more on short-term solutions and may result in sudden rollbacks or abrupt changes in complex organizations, for example in the NSA and its chain of command range of activities. The likelihood of losing competencies is very high. Returning of authorities takes time. Third, cyber security at any cost, illustrated through the NSA scandal, minimizes the US credibility and trustworthiness to international partners, friends, and allies. A perceived disregard to international agreements may lead to diplomatic difficulties. For example, cyber intrusions pertaining to the European Union-US free trade agreement actually harm the agreement, which is in place to protect: the US economy.

The US government has not actually established robust cyber security. Protection against cyber threats means hardening the entire system, especially those that enable a safe critical infrastructure. However, the debate about cyber security has been militarized, which is dominated by terminology of warfare. Additionally, constant warning of cyber threat dangers while struggling in the whole-of-nation-approach creates a dangerous causality. It results in overhype to the offensive and hostile potentials of cyber threats and reduces political understanding to promote the civil led cyber security strategy for the homeland. The Department of Defense is likely not the proper entity to lead civil cyber security efforts.

BIBLIOGRAPHY

Primary Sources

Department of Homeland Security and the Department of Defense. “Memorandum of agreement between the regarding cyber security,” 13 October 2010. http://www.dhs.gov/xlibrary/assets/20101013-dod-dhs-cyber-moa.pdf (accessed 5 February 2014).

Chertoff, Michael, McConnell Mike, Wolfowitz Paul, Cartwright James, Lynn III William, William J. Perry, Richard Clark, and Jamie Gorelick. “Letter to the Majority Leader Reid and Minority Leader Mcconnell.” http://pdfserver.amlaw.com/cc/120119_cyber_letter.pdf (accessed 11 February 2014).

Books

Beer, von Thomas. *Cyberwar: Bedrohung für die Informationsgesellschaft*. Marburg: Tectum - Der Wissenschaftsverlag, 2011.

Borchert, Heiko. *Vernetzte Sicherheit. Leitidee der Sicherheitspolitik im 21*. Jahrhundert. Hamburg, Berlin, Bonn: Mättler, 2004.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. 2nd Edition ed. Beijing: O'Reilly Media, 2011.

Cimbala, Stephen J. *Military Persuasion in War and Policy: The Power of Soft*. Westport, CT: Praeger, 2002.

Clarke, Richard A. and Robert K. Knake. *Cyber War: the Next Threat to National Security and What to Do About It*. New York: Ecco, 2012.

Clausewitz, Carl von. *On War*. Indexed Edition. Reprint ed. Princeton, NJ: Princeton University Press, 1989.

Gaycken, Sandro. *Cyberwar - Das Wettrüsten hat längst begonnen*. München: Verlagsgruppe Random House GmbH, 2012.

Gaycken, Sandro. *Cyberwar: Das Internet als Kriegsschauplatz*. München: Open Source Press, 2011.

Kassimeris, George, and John Buckley. *The Ashgate Research Companion to Modern Warfare*. Farnham, Surrey: Ashgate, 2010.

Kloiber, Manfred, Jan Rähm, and Peter Welchering. *Bits und Bomben : Cyberwar: Konzepte, Strategien und reale digitale Kontroversen*. München: AVM, 2012.

Knox, MacGregor, and Williamson Murray, eds. *The Dynamics of Military Revolution, 1300-2050*. Cambridge, UK: Cambridge University Press, 2001.

Kramer, Franklin D., Stuart H. Starr, and Larry Wentz, eds. *Cyberpower and National Security*. Washington, DC: Potomac Books Inc., 2009.

Libicki, Martin C. *Crisis and Escalation in Cyberspace*. Santa Monica, CA: RAND Corporation, 2012.

_____. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

Nye, Joseph S., and Brent Scowcroft. *Securing Cyberspace: A New Domain for National Security*. Edited by R. Nicholas Burns and Jonathon Price. Washington, DC: Aspen Institute, 2012.

Minkwitz, Olivier. *Ohne Hemmungen in den Krieg?: Cyberwar und die Folgen*. Frankfurt: Hessische Stiftung Friedens- und Konfliktforschung, 2003.

Olson, Parmy. *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency*. London: Random House UK Limited, 2013.

Parks, Raymond C., and David P. Duggan. *"Principles of Cyber-Warfare." Proceedings of the 2001 IEEE workshop on Information and Security*. West Point, NY: US Military Academy, 6 June 2001.

Ranum, Marcus J. *The Myth of Homeland Security*. Indianapolis, IN: Wiley, 2004.

Schmidt-Radefeldt, Roman. *Automatisierung und Digitalisierung des Krieges: Drohnenkrieg und Cyberwar als Herausforderungen für Ethik, Völkerrecht und Sicherheitspolitik*. Forum Innere Führung, Baden-Baden: Nomos, 2012.

Thomas, Timothy L. *Recasting the Russian Star.: Russia Forges Tradition and Technology through Toughness*. Fort Leavenworth, KS: Foreign Military Studies Office (FMSO), 2011.

Tzu, Sun. *The Art of War (History and Warfare)*. Boulder: Basic Books, 1994.

Weiße, Günther K. *Informationskrieg und Cyber War*. Stuttgart: Motorbuch Verlag, 2007.

Governmental and International Papers

Committee on Homeland Security House of Representatives 112th Congress. "Examining the Homeland Security Impact of the Obama Administration´s Cyber Security Proposal." http://www.gpo.gov. http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg72253/pdf/CHRG-112hhrg72253.pdf (accessed 11 February 2014).

Federal Ministry of Interior. "Cyber Security Strategy for Germany." http://www.cio.bund.de. http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile (accessed 11 February 2014).

Information Sharing and Analysis Centers (ISAC). "The Role of Information Sharing and Analysis Centers (ISACs) in Private/public Sector Critical Infrastructure Protection." http://www.isaccouncil.org. http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf (accessed 5 February 2014).

Klimburg, Alexander, ed. *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012. http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf (accessed 13 October 2013).

UK Cabinet Office. "Cyber Security Strategy of the United Kingdom. Safety, Security and Resilience in Cyber Space." http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (accessed 10 January 2014).

US Congress, House. The amendment to the Foreign Intelligence Surveillance Act of 1978. 110th Cong. H. R. 6304. Washington, DC: Government Printing Office, 2008.

US Department of Defense. "Department of Defense Directive O-3600.01." http://www.fas.org/irp/doddir/dod/info_ops.pdf (accessed 5 February 2014).

_____. Joint Publication (JP) 2-01, *Joint and National Intelligence support to Military Operations*, 5 January 2012. http://www.dtic.mil/doctrine/new_pubs/jp2_01.pdf (accessed 5 February 2014).

_____. Joint Publication (JP) 3-13, *Information Operation*, 27 November 2012. "http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed 5 February 2014).

US Department of Homeland Security. *National Infrastructure Protection Plan*. Washington, DC, 2009. http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed 22 October 2013).

_____. "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection." http://www.dhs.gov/homeland-security-presidential-directive-7 (accessed 5 February 2014).

US Government Accountability Office (GAO). Cyber security, a better-defined and implemented national strategy is needed to address persistent challenges, 7 March 2013, http://www.gao.gov/assets/660/652817.pdf (accessed 22 October 2013).

US Government. *Cyber security, Threats Impacting the Nation*, 24 April 2012. http://www.gao.gov/assets/600/590368.pdf (accessed 22 October 2013).

_____. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001. Public Law 107–56—October 26, 2001. Washington, DC: Government Printing Office, 2001.

_____. USA Patriot Act additional reauthorizing amendments act of 2006. Public Law 109–178—March 9, 2006. Washington, DC: Government Printing Office, 2006.

White House. "Presidential Proclamation—Critical Infrastructure Security and Resilience Month, 2013." http://www.whitehouse.gov. http://www.whitehouse.gov/the-press-office/2013/10/31/presidential-proclamation-critical-infrastructure-security-and-resilienc (accessed February 5, 2014).

_____. "Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11737-1144 (February 19, 2013)," https://www.federalregister.gov/articles/

2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity (accessed 4 February 2014).

_____. “Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, 2009.” http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (accessed 5 February 2014).

_____. “Exec. Order No. 13636, Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11737-1144 (19 February 2013).” https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity (accessed 4 February 2014).

_____. “The National Security Strategy of the United States, 2006.” http://georgewbush-whitehouse.archives.gov/nsc/nss/2006/ (accessed February 05, 2014).

_____. “The National Security Strategy of the United States, 2010.” http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf (accessed 5 February 2014).

_____. “The National Strategy to Secure Cyberspace, 2003.” http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (accessed 5 February 2014).

_____. “The Comprehensive National Cybersecurity Initiative, 2009.” http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity- initiative (accessed 5 February 2014).

US Strategic Command. “US Cyber Command.” http://www.stratcom.mil/factsheets/Cyber_Command/ (accessed 5 February 2014).

The United Nations. “Charter of the United Nations and Statute of the International Court of Justice.” https://treaties.un.org/doc/publication/ctc/uncharter.pdf (accessed 11 February 2014).

Journals, Magazine, and Electronic Documents

Bajaj, Kamlesh. The Cybersecurity Agenda: Mobilizing for International Action. New York: EastWest Institute, 2010. http://www.ewi.info/sites/default/files/ideas-files/Bajaj_Web.pdf (accessed 9 March 2014).

Billo, Charles. “Cyber Warfare.” Institute for security technology studies at Dartmouth College, November 2004. http://www.ists.dartmouth.edu/library/212.pdf (accessed 17 November 2013).

Bizeul, David. “Russian Business Network Study.” 20 November 2007. http://www.bizeul.org/files/RBN_study.pdf (accessed 18 November 2013).

Bowman, Steve. “Homeland Security: The Department of Defense’s Role.” http://www.fas.org/man/crs/RL31615.pdf (accessed 5 February 2014).

Burns, Thomas L. “The Origins of the National Security Agency (1940-1952).” http://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf (accessed 5 February 2014).

Cavelty, Myriam Dunn. “Cyber-Security and Threat Politics: US efforts to secure the Information age.” New York: Routledge, 2007. http://www.academia.edu/462492/Cyber-Security_and_Threat_Politics_US_Efforts_to_Secure_the_Information_Age (accessed 19 November 2013).

Cooper, Lane F. “Cyber Security Strategies for the Small Businesses Market.” Solutions for Small Business Reports (2010). http://www.ctam.com/html/sfsb/pdf/Security-White-Paper.pdf (accessed 18 November 2013).

Dean, David et al. “The Connected World: The Digital Manifesto: How Companies and Countries Can Win in the Digital Economy.” Boston Consulting Group Perspectives (BCG), 27 January 2012. https://www.bcgperspectives.com/content/articles/growth_innovation_connected_world_digital_manifesto/ (accessed October 2013).

Denning, Dorothy E. “Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy.” http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf (accessed 12 February 2014).

Eckert, Sue. “Protecting Critical Infrastructure: The Role of the Private Sector.” http://www.ridgway.pitt.edu/Portals/1/pdfs/Publications/Eckert.pdf (accessed 11 February 2014).

Europol. “Threat Assessment (Abridged). Internet Facilitated Organised Crime (iOCTA).” The Hague: Europol, 2011. https://www.europol.europa.eu/sites/default/files/publications/iocta_0.pdf (accessed 18 November 2013).

Evans, Dave. “The Internet of Things. How the Next Evolution of the Internet Is Changing Everything.” San Jose, CA: Cisco Internet Business Solutions Group, 2011. http://www.cisco.com/web/about/ac79/ docs/innov/IoT_IBSG_0411FINAL.pdf (accessed 22 October 2013).

Fahrenkrug, David T. “Countering the Offensive Advantage in Cyberspace: An Integrated Defensive Strategy.” http://www.ccdcoe.org/publications/2012proceedings/3_4_Fahrenkrug_AnIntegratedDefensiveStrategy.pdf (accessed 5 February 2014).

Fenton, Russell. “A combined arms approach to defending Army networks.” http://www.dtic.mil/dtic/tr/fulltext/u2/a577086.pdf (accessed 5 February 2014).

Howe, George F. “The early history of NSA.” http://www.nsa.gov/public_info/_files/cryptologic_spectrum/early_history_nsa.pdf (accessed 5 February 2014).

International Communication Union (ITU). *ITU National Cybersecurity Strategy Guide*. 2011. http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurity StrategyGuide.pdf. (accessed 22 October 2014).

International Organization for Standardization. “ISO/IEC 18028-1. Information Technology—Security Techniques—IT Network Security—Part: 1 Network Security Management.” http://www.pqm-online.com/assets/files/standards/iso-iec_18028-1-2006.pdf (accessed 20 February 2014).

Krekel, Bryan. “Capability of the People’s Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.” http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf (accessed 12 February 2014).

Krepinevich, Andrew. “Cyber Warfare: a 'nuclear option'?” http://www.csbaonline.org/wp-content/uploads/2012/08/CSBA_Cyber_Warfare_For_Web_1.pdf. (accessed 5 February 2014).

Lakoff, George F., and Mark Johnson. “Metaphors We Live By.” http://pages.vassar.edu/theories-of-the-novel/files/2013/04/Metaphors-We-Live-By.pdf (accessed 11 February 2014).

Lambeth, Benjamin S. “Airpower, Spacepower, and Cyberpower.” *Joint Force Quarterly* (JFQ), 2011. http://www.ndu.edu/press/lib/images/jfq-60/JFQ60_46-53_Lambeth.pdf (accessed 12 February 2014).

Langner, Ralph. “To Kill a Centrifuge-a Technical Analysis of What Stuxnet’s Creators Tried to Achieve.” http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf (accessed 11 February 2014).

Lewis, James A. “Cybersecurity and Critical Infrastructure Protection.” Center for Strategic and International Studies. Entry posted January 2006. http://csis.org/files/media/csis/pubs/0601_cscip_preliminary.pdf (accessed 5 February 2014).

Lewis, James A., and Katrina Timlin. “Cybersecurity and Cyberwarfare.” http://www.unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf (accessed 5 February 2014).

Lynn III, William J. “The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack.” *Foreign Affairs*, 28 September 2011, http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later (accessed 18 November 2013).

National Institute of Standards and Technology. “Minimum Security Requirements for Federal Information and Information Systems.” http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf (accessed 11 February 2014).

Panetta, Leon E. “Defending the nation from cyber attack.” *Business Executives for National Security*, New York, 11 October 2012. http://www.bens.org/document.doc?id=188 (accessed 5 February 2014).

Rid, Thomas. “Cyberwar and Peace: Hacking Can Reduce Real-World Violence.” *Foreign Affairs* (November/December 2013): 1. http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace (accessed 4 February 2014).

Schreier, Fred. “On Cyberwarfare.” *DCAF horizon 2015 working paper 7* (2012). http://www.dcaf.ch/Publications/On-Cyberwarfare (accessed 18 November 2013).

Smith, Geoff. “Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.” *OECD paper* (2010). http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf (accessed 18 November 2013).

Tikk, Eneken, Kadri Kaska, and Liis Vihul. “International Cyber Incidents: Legal Considerations.” Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010. http://www.ccdcoe.org/publications/books/legalconsiderations.pdf (accessed 4 February 2014).

US Office of the National Counterintelligence Executive. “Foreign Spies Stealing US Economic Secrets in Cyberspace.” Report to Congress On Foreign Economic Collection and Industrial Espionage, 2009-2011.” http://www.ncix.gov/publications/reports/ fecie_all/Foreign_Economic_Collection_2011.pdf (accessed 11 February 2014).

Wilson, Clay. “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress.” CSR Report for Congress. Washington, DC: Congressional Research Service, 29 January 2008. http://www.fas.org/sgp/crs/terror/RL32114.pdf (accessed 18 November 2013).

Websites and Blogs

“Cyber Spending at Defense.” http://www.nextgov.com/cybersecurity/ 2011/03/cyber-spending-at-defense/48790/ (accessed 19 November 2013).

“US Cybersecurity Spending to Rise.” Homeland Security News Wire.com. http://www. homelandsecuritynewswire.com/us-cybersecurity-spending-rise (accessed 19 November 2013).

Barry, Tom. “Synergy in Security: The Rise of the National Security Complex.” http://www. dollarsandsense.org/archives/2010/0310barry.html (accessed 19 November 2013).

Censer, Marjorie, and Tom Temin. “The Cybersecurity Boom.” *Washington Post*, 10 May 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/05/07/ AR2010050704503.html (accessed 19 November 2013).

Cole, August, and Siobhan Gorman. “Defense Firms Pursue Cyber-Security Work.” *Wall Street Journal*. Entry posted 18 March 2009. http://online.wsj.com/news/articles/ SB123733224282463205 (accessed 19 November 2013).

DER SPIEGEL. “NSA Spying Scandal.” http://www.spiegel.de/international/topic/ nsa_spying_scandal/ (accessed 5 February 2014).

Homeland Security News Wire. “US Cybersecurity Spending to Rise.” http://www.homeland securitynewswire.com/us-cybersecurity-spending-rise (accessed 11 February 2014).

ICS-CERT year in review — 2012. https://ics-cert.us-cert.gov. http://www.uscg.mil/hq/cg5/cg544/docs/Year_in_Review_FY2012_Final.pdf (accessed 5 February 2014).

Information Sharing and Analysis Centers (ISAC). "The Role of Information Sharing and Analysis Centers (ISACs) in Private/public Sector Critical Infrastructure Protection." http://www.isaccouncil.org/images/ISAC_Role_in_CIP.pdf (accessed 5 February 2014).

ISO/IEC 27032:2012. "Information Technology—Security Techniques—Guidelines for Cybersecurity." http://www.iso27001security. com/html/27032.html (accessed 11 February 2014).

Lemos, Robert. "DHS video shows potential impact of cyberattack." Entry posted 27 September 2007. http://www.securityfocus.com/brief/597 (accessed 21 November 2013).

Leyden, John. "US and UK Gov Cyber Defences = Big Boys' Trough-Slurp." Entry posted 22 October 2010. http://www.theregister.co.uk/2010/10/22/firewall_guru_interview/ (accessed 19 November 2013).

Lohrmann, Dan. "New Cybersecurity Technology Alliance Points the Way. Entry posted 13 November 2009. http://www.govtech.com/blogs/lohrmann-on-cybersecurity/New-Cyber-Security-Technology.html (accessed 19 November 2013).

Nextgov. "Cyber Spending at Defense." http://www.nextgov.com/cybersecurity/2011/03/cyber-spending-at-defense/48790/ (accessed 11 February 2014).

Paganinip, Pierluigi. "Hacktivism: Means and Motivations … What Else?" Entry posted 2 October 2013. http://resources.infosecinstitute.com/hacktivism-means-and-motivations-what-else/ (accessed 12 February 2014).

_____. "Why Humans Could Be the Weakest Link in Cyber Security Chain?" *Security Affairs*, 3 October 2012. http://securityaffairs.co/wordpress/9076/social-networks/why-humans-could-be-the-weakest-link-in-cyber-security-chain.html (accessed 18 November 2013).

Ricdela, Aaron. "Symantec, Mcafee, Checkpoint Await Spending Surge." Entry posted 18 January 2010. http://www.businessweek.com/technology/content/jan2010/tc20100115_453540.htm (accessed 19 November 2013).

Rogers, Mike. "US business are in an unfair fight against cyberthreats." My opinions. Entry posted 23 October 2013. http://www.washingtonpost.com/opinions/mike-rogers-us-businesses-are-in-an-unfair-fight-against-cyberthreats/2013/10/22/5a5167b8-3b32-11e3-b6a9-da62c264f40e_story.html (accessed 5 February 2014).

US Department of Defense. "The Pentagon's New Cyber Strategy." http://www.defensenews.com/print/article/20110818/C4ISR02/108180316/The-Pentagon-s-new-cyber-strategy (accessed 11 February 2014).